Contents

1 Overview of Wireless Security, Attack and Defense 1
1.1 Overview of Wireless Security 1
1.1.1 Origin of Wireless Security 1
1.1.2 Difference Between Wireless Security and Mobile Security 2
1.1.3 Status Quo of Wireless Security 2
1.2 Wireless Attack and Defense Methods 3
1.2.1 Common Attack Targets 3
1.2.2 Wireless Attack Methods 4
1.2.3 Wireless Defense Methods 5
1.2.4 Trend of Wireless Security 5

2 Tools for Wireless Security Research 7
2.1 Software-Defined Radio Technology 7
2.1.1 SDR Capabilities 8
2.1.2 SDR Usage 9
2.2 SDR Hardware Tools 10
2.2.1 USRP 10
2.2.2 RTL-SDR 12
2.2.3 HackRF 23
2.2.4 BladeRF 25
2.2.5 SDR Software Tool—GNU Radio 37
2.2.6 GNU Radio Installation 38
2.2.7 The First Thing to Do After Installation 45
2.2.8 Example: OFDM Tunnel 50
2.2.9 Sniff Mouse and Keyboard Data 57
Further Reading 70

Bibliografische Informationen
http://d-nb.info/1150794682

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3 RFID/NFC Security 71
3.1 Introduction to Mifare Classic 72
3.2 Security Analysis of Mifare Classic 73
3.2.1 Review of the Process of Cracking Mifare Classic 73
3.3 A Real Case of Cracking Mifare Classic 76
3.3.1 Introduction to Proxmark III 76
3.3.2 Burn and Use Proxmark III Firmware 77
3.3.3 Proxmark III Client 82
3.3.4 Test the Security of Mifare Classic with Proxmark III 84
3.3.5 Introduction to Chameleon-Mini 90
3.3.6 Burn and Use Chameleon-Mini Firmware 92
3.3.7 Simulate Mifare Classic by Combining Proxmark III and Chameleon-Mini 95
3.3.8 Conclusion of HF Attack and Defense 98
3.4 Security Analysis of LFID Cards 98
3.4.1 Introduction to LFID Cards 98
3.4.2 Coding Principle of ID Cards 100
3.4.3 Decoding Principle of ID Cards 100
3.4.4 Read Data from ID Cards 101
3.4.5 Format of the ID Card Number 102
3.5 Clone an LFID Card 103
3.5.1 Simulation Attacks with Proxmark III 104
3.5.2 Clone Attacks with a Blank Card 106
3.5.3 Simulation Attacks with HackID 107
3.6 EMV Privacy Leakage 108
3.6.1 EMV Introduction 108
3.6.2 Mechanism of Privacy Leakage in Contactless Chip Cards 109
3.6.3 Phenomenon of Privacy Leakage in Contactless Chip Cards 113
3.6.4 Contactless Chip Card Fraud 114
3.6.5 Privacy Protection in the Use of Contactless Chip Cards 118
Further Reading 121

4 433/315 MHz Communication 123
4.1 Sniff and Analyze the Security of Remote Control Signals 123
4.2 Attacks by Replaying Remote Control Signals 125
4.2.1 Parking Bar Signal Replay 125
4.2.2 Wireless Door Bell Signal Replay 130
4.2.3 Vibrator Signal Replay 133

4.3 Crack Fixed-Code Garage Doors with Brute Force 143
4.3.1 Complexity of Brute-Force Attack 143
4.3.2 Hardware for Fixed-Code Brute-Force Attack 146
4.4 Security Analysis of Remote Car Key Signals 147
4.4.1 Generation of Remote Control Signals 151
4.4.2 Security Analysis of Keeloq Key Generation Algorithm 154
4.4.3 An Example of Remote Controller Bugs 157
4.4.4 Rolljam Replay Attacks on Car Keys 161
4.5 Security Analysis of the PKE System 162
4.6 Security Analysis of the Tire Pressure Monitoring System 165
Further Reading 171

5 Aeronautical Radio Navigation 173
5.1 Introduction to ADS-B System 173
5.1.1 Definition of ADS-B 174
5.1.2 Definition of 1090ES 175
5.2 ADS-B Signal Encoding 175
5.2.1 Modulation Method 176
5.2.2 Format of Message 176
5.2.3 Altitude Code 178
5.2.4 CPR Longitude and Latitude Code 178
5.2.5 CRC Validation 180
5.3 ADS-B Signal Sniffing 181
5.3.1 Receive ADS-B Signal with "Dump1090" 181
5.3.2 Receive ADS-B Signal with "gr-air-modes" 183
5.4 ADS-B Signal Deception 187
5.5 Analysis of Attack and Defense 188
Further Reading 193

6 Bluetooth Security 195
6.1 Introduction to Bluetooth Technology 195
6.2 Bluetooth Sniffing Tool Ubertooth 198
6.2.1 Ubertooth Software Installation 198
6.2.2 Ubertooth Usage 203
6.3 Low-Power Bluetooth 212
6.3.1 TI's BLE Sniffer 213
6.3.2 Sniff BTLE Data Packets with "Ubertooth-Btle" 216
6.3.3 Read and Write BLE Devices' Properties with a Mobile App 220
6.3.4 Transmit Data Packets by Simulating the BLE Device 222
Further Reading 226

7 **ZigBee Technology** ... 227
7.1 Introduction to ZigBee ... 227
7.1.1 The Relationship Between ZigBee and IEEE 802.15.4 ... 228
7.1.2 Structure of 802.15.4 Frames ... 228
7.1.3 Different Types of MAC Frame in ZigBee ... 230
7.1.4 Device Types and Network Topology of ZigBee ... 230
7.1.5 ZigBee Networking ... 232
7.1.6 Application Layer of ZigBee ... 232
7.1.7 The Application Support Sub-layer of ZigBee ... 233
7.1.8 Application Profile of ZigBee ... 234
7.2 ZigBee Security ... 234
7.2.1 Security Layers ... 235
7.2.2 Key Types ... 236
7.2.3 Security Levels ... 237
7.2.4 Key Distribution ... 238
7.2.5 Access Authentication for ZigBee Nodes ... 239
7.3 ZigBee Attacks ... 239
7.3.1 Attacking Tools ... 239
7.3.2 Protocol Analysis Software ... 241
7.3.3 Network Discovery ... 243
7.3.4 Attack an Unencrypted Network ... 245
7.3.5 Attack an Encrypted Network ... 250
7.4 An Example of Attacking ... 252
7.4.1 Obtain the Key from the Device ... 253
7.4.2 Attacks by Using the Key ... 257
7.5 Summary of Attacks and Defenses ... 265
Further Reading ... 265

8 **Mobile Network Security** ... 267
8.1 Security Status of the GSM System ... 267
8.1.1 Terminology and Basic Concepts of the GSM/UMTS System ... 267
8.1.2 Security of GSM Encryption Algorithms ... 271
8.1.3 Active Attack and Passive Attack in GSM ... 274
8.1.4 GSM Sniffing with “gr-gsm” ... 280
8.2 IMSI Catcher ... 298
8.2.1 What Is an IMSI Catcher? ... 298
8.2.2 IMSI Catcher in GSM Environment ... 299
8.2.3 IMSI Catcher in UMTS Environment ... 301
8.2.4 IMSI Catcher in LTE Environment ... 303

8.2.5 Defect of the IMSI Catcher 308
8.2.6 Stingray Cellphone Tracker 309
8.2.7 IMSI Catcher Detector 311
8.3 Femtocell Security 314
8.3.1 Introduction to Femtocell 314
8.3.2 Attack Surface of Femtocell 315
8.3.3 GSM Femtocell Based on VxWorks 316
8.4 LTE Redirection and Downgrade Attack 321
8.4.1 Redirection Attack Principles 322
8.4.2 The Cause of Redirection Bugs 328
8.5 'Ghost Telephonist' Attack 330
8.5.1 Vulnerability Principle 333
8.5.2 Experiment Setting 335
8.5.3 Attack Methods 336
8.5.4 Countermeasures 340
8.6 Analysis of Attack and Defense. 342
Further Reading 342

9 Satellite Communication 343
9.1 Overview of Artificial Satellites. 343
9.2 GPS Security Research 344
9.2.1 GPS Sniffing and Security Analysis 344
9.2.2 GPS Spoofing 346
9.2.3 Methods of Defense and Suggestions 358
9.3 Security Analysis of Globalstar System 361
9.3.1 Globalstar's CDMA Technology 362
9.3.2 Globalstar Data Cracking 363
9.3.3 Possible Attack Methods 367
Further Reading 368